10 étapes pour mettre en œuvre un programme défendable de gestion des risques liés aux tiers

1. Définir et décrire clairement l'étendue de la tolérance au risque de l'organisation.

Tenez compte du secteur et des diverses juridictions dans lesquelles votre entreprise opère en ce qui concerne le seuil de tolérance au risque propre à l'entreprise. Existe-t-il des risques spécifiques inhérents à la conduite d'activités dans un secteur économique, un pays ou une région particulier(e) ? L'entreprise a-t-elle soigneusement identifié ces risques lors du processus d'évaluation des risques ? Quelles mesures d'atténuation ou autres mesures de précaution l'entreprise a-t-elle convenu de mettre en œuvre pour faire face à ces risques ?

2. Préparer et adopter une politique de gestion des risques liés aux tiers (TPRM) qui définit la procédure que l'organisation utilisera pour vérifier correctement, intégrer et, si nécessaire, désengager les fournisseurs.

L'organisation doit adopter une politique spécifique qui sert de base à la gestion des risques liés aux tiers dans l'ensemble de l'organisation et de ses différentes unités opérationnelles. **La politique doit détailler le processus utilisé par l'organisation pour *identifier, filtrer, sélectionner, évaluer et surveiller* les fournisseurs potentiels.**

Idéalement, la politique TPRM doit également *inclure un code d'éthique ou de conduite pour les partenaires commerciaux (le Code).* À un niveau très élevé, le Code doit définir les attentes de l'organisation en matière de conduite acceptable. Tous les tiers avec lesquels l'organisation passe des contrats doivent être tenus d'observer le Code. Toute violation du Code doit constituer un motif immédiat de résiliation du contrat.

La politique TPRM doit également établir clairement *les rôles et les responsabilités*. Cela inclut l'identification des unités commerciales ou des individus qui seront responsables de l'exécution de certains éléments de la politique, tels que la sélection du fournisseur, le filtrage initial des parties refusées, les négociations contractuelles, l'audit/l'inspection, le renouvellement et la résiliation, etc.

3. Attribuez une note de risque à chaque tiers en utilisant une échelle appropriée.

Une échelle TPRM doit clairement séparer les risques en trois catégories principales – risque *élevé, risque moyen et risque faible* - et s'appuyer sur des critères objectifs pour aider la fonction de conformité à identifier les risques les plus critiques auxquels l'organisation est confrontée de manière globale.

Des ressources tierces, telles que l'indice de perception de la corruption (« IPC ») de Transparence International, peuvent rationaliser ce processus en ce qui concerne des domaines particuliers. Un score composite, tenant compte de la vue complète des risques que l'organisation identifie comme pertinents, doit ensuite être calculé pour chaque fournisseur. La discrétion est cruciale pour s'assurer que seul un faible pourcentage des risques est effectivement classé comme à risque élevé, ce qui permet à l'entreprise d'affecter plus efficacement les ressources aux mesures d'atténuation des risques.

4. Dans la mesure du possible, cartographiez l'ensemble de la chaîne d'approvisionnement de l'entreprise pour maximiser la visibilité sur l'ensemble du cycle de vie du produit/service et identifier visuellement où se situent les risques les plus importants.

Bien que cela puisse sembler une tâche fastidieuse, collaborer avec des parties prenantes internes compétentes pour comprendre les contributions des différents tiers au cycle de vie des produits/services de l'entreprise est un élément indispensable de la pratique TPRM contemporaine. C'est particulièrement vrai lorsque l'entreprise peut être soumise à des régimes réglementaires tels que la directive de l'Union européenne sur la diligence raisonnable en matière de durabilité des entreprises, la loi allemande sur la chaîne d'approvisionnement ou la loi uyghure sur la prévention du travail forcé, entre autres.

Dans chaque cas, la cartographie de la chaîne d'approvisionnement est requise pour identifier le non-respect des normes environnementales et/ou des droits de l'homme prescrites. D'un point de vue du risque d'entreprise, la cartographie peut également aider l'organisation à identifier et à traiter concrètement les vulnérabilités opérationnelles qui pourraient découler de la dépendance à un tiers particulier.

5. Sélectionner et mettre en œuvre un système TPRM automatisé à utiliser dans le cadre de l'administration du programme TPRM.

Pour toutes les organisations, la gestion des relations avec des tiers nécessite l'utilisation d'une **solution TPRM automatisée** qui consolide les fonctions d'administration TPRM sur une seule plateforme. La dépendance aux processus manuels est à la fois insuffisante et peu susceptible de répondre aux attentes actuelles des organismes de réglementation, ce qui met considérablement l'accent sur la capacité de l'organisation à mener une diligence raisonnable, à administrer une formation, à tirer parti des audits, à délivrer des certifications de conformité et à aligner efficacement les risques d'entreprise et de conformité.

Cela nécessite l'adoption d'une solution automatisée telle que le système d'information sur la gouvernance, les risques et la conformité NAVEX One (GRC-IS), qui permet à la fonction de conformité d'intégrer, de filtrer, de hiérarchiser et de surveiller les informations sur les risques des fournisseurs en temps réel.

6. Examiner toutes les formes standard d'accords généralement utilisés avec les fournisseurs de l'organisation pour intégrer les principaux engagements, déclarations et garanties de conformité.

Un élément clé d'un TPRM efficace est la délimitation de normes contractuelles claires dans le contexte de tout accord définitif conclu entre l'organisation contractante principale et le partenaire tiers.

En plus d'être lié par le Code de l'organisation, le contrat lui-même doit exiger que le tiers autorise l'audit et l'inspection de ses livres et registres après un préavis raisonnable. Le contrat doit également prévoir l'invocation de droits de résiliation en cas de non-respect par le tiers du Code ou de toute disposition substantielle de l'accord définitif exigeant le respect de lois ou règlements particuliers.

7. Envisagez de fournir une formation à des partenaires tiers dans les domaines les plus préoccupants.

La fourniture de formations à des tiers est un moyen pratique de souligner que l'entreprise contractante principale prend ses obligations de conformité au sérieux. À cette fin, l'organisation peut proposer une formation à ses partenaires tiers dans les domaines à risque les plus élevés identifiés pendant le processus de sélection et d'intégration des tiers. Par exemple, dans un pays dont le score IPC est inférieur à la moyenne (indiquant une corruption systémique), une formation ciblée sous la forme d'une exposition aux principes de lutte contre la corruption (ABAC) renforcerait le message selon lequel l'entreprise n'a aucune tolérance pour les tentatives illégales d'influencer des tiers par le paiement de pots-de-vin ou l'octroi de cadeaux.

8. S'assurer que les tiers sont en mesure de signaler les violations du Code de l'organisation ou d'autres infractions éthiques et légales.

Dans la mesure du possible, les entreprises doivent envisager de tirer parti de leur système de signalement des incidents existant pour permettre aux parties externes – y compris les employés de tout partenaire commercial – de signaler des questions impliquant une violation du Code ou d'autres infractions éthiques et/ou légales par les employés, les sous-traitants et les agents de l'entreprise. Cette capacité de reporting est de plus en plus requise par les systèmes réglementaires axés sur la transparence de la chaîne d'approvisionnement.

9. Empêcher, dans la mesure du possible, la fragmentation des informations tierces.

Le plus grand défi auquel les entreprises contemporaines sont peut-être confrontées est la consolidation des silos d'informations existants. Pour être efficaces, toutes les informations relatives à un tiers particulier doivent être stockées dans un emplacement unique et largement accessible aux principales parties prenantes de l'organisation. L'accès à un fichier complet contenant les informations sur les fournisseurs est essentiel pour maintenir un profil de risque fiable.

10. Examiner et mettre à jour périodiquement les politiques et procédures TPRM à la lumière des évolutions réglementaires et des enseignements tirés.

Il va de soi que l'organisation doit revoir régulièrement ses propres politiques et procédures relatives au TPRM pour apporter des améliorations basées sur les enseignements tirés et sur les attentes réglementaires émergentes. Pour optimiser l'efficacité du programme TPRM, les politiques et procédures doivent être révisées au moins une fois par an, voire plus tôt, afin de déterminer si des modifications sont nécessaires.